SECTION I—CLAIMS

Amendment to the Claims:

This listing of the claims will replace all prior versions and listings of claims in the application. Claims 1, 4, 6-7, 10, 12-14, 16, 18-19, 21, 23, 26, 28-30, and 32 are amended herein. Claims 5, 11, 15, 17, 20, 22, 27, 31, and 33 are herein canceled without prejudice. New claims 34-42 are presented herein. Claims 1-4, 6-10, 12-14, 16, 18-19, 21, 23-26, 28-30, 32, and 34-42 remain pending in the application.

Listing of the Claims:

1. (Currently Amended) A method performed by a user terminal of a wireless access network, the method comprising:

scrambling a user terminal certificate using a first portion of a shared secret to be known only by the user terminal and an access point of the wireless access network, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key;

disqualifying the first portion of the shared secret from use with symmetric key cryptography between the user terminal and the access point;

generating an authenticator string including data encrypted with the user terminal private key; and

sending a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.

2. (Original) The method of claim 1, further comprising generating the shared secret and providing the shared secret to the access point.

3. (Previously presented) The method of claim 2, wherein providing the shared secret to the access point comprises encrypting the shared secret with an access point public key.

4. (Currently Amended) The method of claim 1, wherein scrambling the user terminal certificate using the first portion of the shared secret comprises combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with the first portion ~~a part~~ of the shared secret.

5. (Canceled).

6. (Currently amended) The method of claim 1 [[5]], wherein the remaining[[der]] portion of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

7. (Currently Amended) A user terminal comprising:

a memory to store a user terminal private key and a user terminal certificate, the user terminal certificate including a user terminal public key which corresponds to the user terminal private key;

a processor coupled to the memory to scramble the user terminal certificate using a first portion of a shared secret to be known only by the user terminal and an access point of [[the]] a wireless access network and to generate an authenticator string including data encrypted with the user terminal private key, wherein the first portion of the shared secret to be disqualified from use with symmetric key cryptography between the user terminal and the access point; and

a transmitter coupled to the processor to send a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.

8. (Previously presented) The user terminal of claim 7, wherein the processor also generates the shared secret and the transmitter also provides the shared secret to the access point.

9. (Previously presented) The user terminal of claim 8, wherein the transmitter provides the shared secret to the access point by encrypting the shared secret with an access point public key.

10. (Currently amended) The user terminal of claim 7, wherein the processor scrambles the user terminal certificate using the first portion of the shared secret by combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with the first portion ~~a part~~ of the shared secret.

11. (Canceled).

12. (Currently amended) The user terminal of claim 7 [[11]], wherein the remaining[[der]] portion of the shared secret to be [[is]] used for symmetric key cryptography between the user terminal and the access point.

13. (Currently Amended) A method performed by an access point of a wireless access network, the method comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, an authenticator string including data encrypted with a user terminal private key, and a user terminal certificate scrambled using the shared secret, the scrambled user terminal certificate including a user terminal public key which corresponds to the user terminal private key;

decrypting the shared secret using an access point private key;

unscrambling the user terminal certificate using a first portion of the decrypted shared secret; [[and]]

disqualifying the first portion of the decrypted shared secret from use with symmetric key cryptography between the user terminal and the access point; and

decrypting the authenticator string using the user terminal public key.

14. (Currently Amended) The method of claim 13, wherein unscrambling the user terminal certificate using the first portion of the decrypted shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with the first portion ~~a part~~ of the decrypted shared secret.

15. (Canceled).

16. (Currently amended) The method of claim 13 [[15]], wherein the remaining[[der]] portion of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

17. (Canceled).

18. (Currently Amended) An access point comprising:

a receiver to receive a message from a user terminal, the message containing a shared secret encrypted with an access point public key, an authenticator string including data encrypted with a user terminal private key, and a user terminal certificate scrambled using the shared secret, the user terminal certificate including a user terminal public key which corresponds to the user terminal private key; and

a processor coupled to the receiver to decrypt the shared secret using an access point private key, unscramble the user terminal certificate using a first portion of the decrypted shared secret, and decrypt the authenticator string using the user terminal public key, wherein the first portion of the decrypted shared secret to be disqualified from use with symmetric key cryptography between the user terminal and the access point.

19. (Currently Amended) The access point of claim 18, wherein the processor unscrambles the user terminal certificate using the first portion of the shared secret by combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with the first portion ~~a part~~ of the decrypted shared secret.

20. (Canceled).

21. (Currently amended) The access point of claim 18 [[20]], wherein the remaining[[der]] portion of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

22. (Canceled).

23. (Currently Amended) A machine-readable medium storing data representing instructions that, when performed by a processor of a user terminal, causes the processor to perform operations comprising:

scrambling a user terminal certificate using a first portion of a shared secret to be known only by the user terminal and an access point of [[the]] a wireless access network, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key;

disqualifying the first portion of the shared secret from use with symmetric key cryptography between the user terminal and the access point;

generating an authenticator string including data encrypted with the user terminal private key; and

sending a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.

24. (Original) The machine-readable medium of claim 23, wherein the instructions further cause the processor to perform operations comprising generating the shared secret and providing the shared secret to the access point.

25. (Previously presented) The machine-readable medium of claim 24, wherein providing the shared secret to the access point comprises encrypting the shared secret with an access point public key.

26. (Currently amended) The machine-readable medium of claim 23, wherein scrambling the user terminal certificate using the first portion of the shared secret comprises combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with ~~a part~~ the first portion of the shared secret.

27. (Canceled).

28. (Currently amended) The machine-readable medium of claim 23 [[27]], wherein the remaining[[der]] portion of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

29. (Currently Amended) A machine-readable medium storing data representing instructions that, when performed by a processor of an access point, causes the processor to perform operations comprising:

receiving a message from a user terminal of [[the]] a wireless access network, the message containing a shared secret encrypted with an access point public key, an authenticator string including data encrypted with a user terminal private key, and a user terminal certificate scrambled using a first portion of the shared secret, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key;

decrypting the shared secret using an access point private key;

unscrambling the user terminal certificate using the first portion of the decrypted shared secret;

disqualifying the first portion of the decrypted shared secret from use with symmetric key cryptography between the user terminal and the access point; and

decrypting the authenticator string using the user terminal public key.

30. (Currently amended) The machine-readable medium of claim 29, wherein unscrambling the user terminal certificate using the first portion of the decrypted shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with ~~a part~~ the first portion of the decrypted shared secret.

31. (Canceled).

32. (Currently amended) The machine-readable medium of claim 29 [[31]], wherein the remaining[[der]] portion of the decrypted shared secret is used for symmetric key cryptography between the user terminal and the access point.

33. (Canceled).

34. (New) An apparatus comprising:

a memory to store a certificate;

a processor coupled to the memory to scramble the certificate using a first portion of a shared secret to be known only by the apparatus and an access point of a wireless access network, wherein the first portion of the shared secret to be disqualified from use with symmetric key cryptography with the access point; and

a transmitter coupled to the processor to send a message to the access point, the message including the scrambled certificate.

35. (New) The apparatus of claim 34, wherein the processor also generates the shared secret and the transmitter also provides the shared secret to the access point.

36. (New) The apparatus of claim 35, wherein the transmitter provides the shared secret to the access point by encrypting the shared secret with an access point public key.

37. (New) The apparatus of claim 34, wherein the processor scrambles the certificate using the first portion of the shared secret by combining the certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with the first portion of the shared secret.

38. (New) The apparatus of claim 34, wherein a second portion of the shared secret to be used for symmetric key cryptography with the access point.

39. (New) An access point comprising:

a receiver to receive a message, the message comprising a shared secret encrypted with an access point public key and a certificate scrambled using the shared secret; and

a processor coupled to the receiver to decrypt the shared secret using an access point private key, and unscramble the certificate using a first portion of the decrypted shared secret, wherein the first portion of the decrypted shared secret to be disqualified from use with symmetric key cryptography with the access point.

40. (New) The access point of claim 39, wherein the processor unscrambles the certificate using the first portion of the shared secret by combining the scrambled certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with the first portion of the decrypted shared secret.

41. (New) The access point of claim 39, wherein a second portion of the shared secret is used for symmetric key cryptography with the access point.

42. (New) The access point of claim 39, wherein the certificate includes an identification of a sending apparatus and a sending apparatus public key which corresponds to a sending apparatus private key, wherein the access point authenticates the sending apparatus by checking the certificate.